Risk Assessment Scoring Definitions

	Impact to the Organization			Vulnerability		Controls
Score	**Mission/Reputation**	**Financial**	**Legal**	**Likelihood of Risk**	**Detectability**	**Controls**
1	Little or no mission risk at DMH or Contractors	Loss of less than "x% or $ amount" that incrementally increases as risk increases.	Technical violation of law or regulation. Little or no fine probable.	Low risk, unlikely to occur. Historical and industry show low likelihood of occurrence.	Failures are likely to be detected. Process is directly supervised. Automated safeguards for identifying violations/errors.	Internal and/or automated controls proven to be highly effective in mitigating all risk.
2	Slight mission risk. Possible bad press but no significant patient, physician, or constituent consequences.	Loss of between "x% or $ amounts"	Civil fines and/or penalties up to $100,000 possible, but little risk of exclusion, corporate integrity agreement (CIA), or loss of accreditation/licensure.	Slight risk, historical industry experience shows some likelihood however not experienced in organization to date; simple well understood process; competency demonstrated – less likely to fail.	Slight risk that failure will be detected – process failures; moderate safeguard in place; partially automated process with moderate management oversight.	Routinely audited and/or tested. Performance metrics are established, routinely reviewed and shown little variation. Current policies and procedures exist. Employee training and competency established. Well prepared to manage this risk appropriately based on implemented risk management plans.
3	Moderate mission risk. Probable bad press. Probable modest physician, patient and/or constituent fallout.	Loss of between "x% of $ amounts"	Civil fines and/or penalties up to $1,000,000 probable. Modest risk of exclusion, CIA possible.	Moderate risk of occurrence within the next 12 months; isolated to a single facility.	Moderate risk that failure will not be detected. Limited safeguards in place to identify failure prior to occurrence. Partially automated process with limited management oversight.	Periodically audited and/or tested. Corrective action plans developed and tested for effectiveness. Limited performance metrics established. Risk management plans expected to manage the risks appropriately.

	Impact to the Organization			Vulnerability		Controls
Score	**Mission/Reputation**	**Financial**	**Legal**	**Likelihood of Risk**	**Detectability**	**Controls**
4	Significant negative press coverage. Significant patient, physician, and/or constituent fallout.	Loss of between "x% or $ amounts"	Civil fines and/or penalties up to $1,000,000 probable. Loss of business unit licensure/accreditation. Exclusion possible. CIA probable.	Significant risk; likelihood of occurrence in up to 50% of facilities; complex and/or manual process.	Significantly difficult to detect prior to failure; manual safeguards in place to identify failures; no automated processes; periodic management oversight.	Management Review and approval required. Process not audited or tested or infrequently audited or tested. Limited policy or procedure guidance. Some risk management plans or steps undertaken; not reasonably expected to manage the risk appropriately or fully.
5	Extensive and prolonged negative press coverage. Significant sponsor/board questions of management. Extensive patient, physician, and/or constituent fallout.	Loss of greater than "x% or $ amount"	Criminal conviction and/or exclusion of program or services probable. Fines, penalties, and or legal exposure in excess of 1% of net revenue CIA certain.	High risk of occurrence. Likely to occur in the next 12 months. Highly complex process with numerous handoffs. Relies on extensive specialized skills. Note: Should assume natural/manmade disasters are likely to occur in the next year.	Extremely hard to detect prior to failure. Highly automated with little or no human intervention, oversight or control. No built-in safeguards, cross checks, or other mechanisms to identify error/failures prior to submission/completion.	No formal controls in place. No risk management plans or steps in place currently.